

investigations, the record will be reviewed to determine that granting an access authorization or renewal of access authorization will not endanger the common defense and security and is clearly consistent with the national interest. If this determination is made, access authorization will be granted or renewed. If the NRC is the CSA, questions as to initial or continued eligibility will be determined in accordance with part 10 of chapter I. If another agency is the CSA, that agency will, under the requirements of the NISPOM, have established procedures at the facility to resolve questions as to initial or continued eligibility for access authorization. These questions will be determined in accordance with established CSA procedures already in effect for the facility.

(b) The CSA must be promptly notified of developments that bear on continued eligibility for access authorization throughout the period for which the authorization is active (e.g., persons who marry subsequent to the completion of a personnel security packet must report this change by submitting a completed NRC Form 354, "Data Report on Spouse" or equivalent CSA form).

(c)(1) Except as provided in paragraph (c)(2) of this section, NRC "Q" and "L" access authorizations must be renewed every five years from the date of issuance. An application for renewal must be submitted at least 120 days before the expiration of the five year period, and must include:

(i) A statement by the licensee or other person that the individual continues to require access to classified National Security Information or Restricted Data; and

(ii) A personnel security packet as described in §25.17(d).

(2) Renewal applications and the required paperwork are not required for individuals who have a current and active access authorization from another Federal agency and who are subject to a reinvestigation program by that agency that is determined by the NRC to meet the NRC's requirements. (The DOE Reinvestigation Program has been determined to meet the NRC's requirements). For these individuals, the submission of the SF-86 by the licensee or

other person to the other government agency pursuant to their reinvestigation requirements will satisfy the NRC renewal submission and paperwork requirements, even if less than five years has passed since the date of issuance or renewal of the NRC "Q" or "L" access authorization. Any NRC access authorization continued in response to the provisions of this paragraph will, thereafter, not be due for renewal until the date set by the other government agency for the next investigation of the individual pursuant to the other agency's reinvestigation program. However, the period of time for the initial and each subsequent NRC "Q" or NRC "L" renewal application to the NRC may not exceed seven years. Any individual who is subject to the reinvestigation program requirements of another Federal agency but, for administrative or other reasons, does not submit reinvestigation forms to that agency within seven years of the previous submission, shall submit a renewal application to the NRC using the forms prescribed in §25.17(d) before the expiration of the seven-year period.

(3) If the NRC is not the CSA, reinvestigation program procedures will be set by the CSA.

[62 FR 17688, Apr. 11, 1997]

#### **§25.23 Notification of grant of access authorization.**

The determination to grant or renew access authorization will be furnished in writing to the licensee or organization that initiated the request. Upon receipt of the notification of original grant of access authorization, the licensee or organization shall obtain, as a condition for grant of access authorization and access to classified information, an executed "Classified Information Nondisclosure Agreement" (SF-312) from the affected individual. The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization shall execute a SF-312 before being granted access to classified information. The licensee or other organization shall forward the executed SF-312 to the CSA for retention. If the employee refuses to execute the SF-312, the licensee or

other organization shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date. The individual shall also be given a security orientation briefing in accordance with §95.33 of this chapter. Records of access authorization grant and renewal notification must be maintained by the licensee or other organization for three years after the access authorization has been terminated by the CSA. This information may also be furnished to other representatives of the Commission, to licensees, contractors, or other Federal agencies. Notifications of access authorization will not be given in writing to the affected individual except:

(a) In those cases in which the determination was made as a result of a Personnel Security Hearing or by Personnel Security Review Examiners; or

(b) When the individual also is the official designated by the licensee or other organization to whom written NRC notifications are forwarded.

[62 FR 17688, Apr. 11, 1997]

**§ 25.25 Cancellation of requests for access authorization.**

When a request for an individual's access authorization or renewal of access authorization is withdrawn or canceled, the requestor shall notify the CSA immediately by telephone so that the full field investigation, National Agency Check with Credit Investigation, or other personnel security action may be discontinued. The requestor shall identify the full name and date of birth of the individual, the date of request, and the type of access authorization or access authorization renewal requested. The requestor shall confirm each telephone notification promptly in writing.

[62 FR 17689, Apr. 11, 1997]

**§ 25.27 Reopening of cases in which requests for access authorizations are canceled.**

(a) In conjunction with a new request for access authorization (NRC Form 237 or CSA equivalent) for individuals whose cases were previously canceled,

new fingerprint cards (FD-257) in duplicate and a new Security Acknowledgment (NRC Form 176), or CSA equivalent, must be furnished to the CSA along with the request.

(b) Additionally, if 90 days or more have elapsed since the date of the last Questionnaire for Sensitive Positions (SF-86), or CSA equivalent, the individual must complete a personnel security packet (see §25.17(d)). The CSA, based on investigative or other needs, may require a complete personnel security packet in other cases as well. A fee, equal to the amount paid for an initial request, will be charged only if a new or updating investigation by the NRC is required.

[62 FR 17689, Apr. 11, 1997]

**§ 25.29 Reinstatement of access authorization.**

(a) An access authorization can be reinstated provided that:

(1) No more than 24 months has lapsed since the date of termination of the clearance;

(2) There has been no break in employment with the employer since the date of termination of the clearance;

(3) There is no known adverse information;

(4) The most recent investigation must not exceed 5 years (Top Secret, Q) or 10 years (Secret, L); and

(5) The most recent investigation must meet or exceed the scope of the investigation required for the level of access authorization that is to be reinstated or granted.

(b) An access authorization can be reinstated at the same, or lower, level by submission of a CSA-designated form to the CSA. The employee may not have access to classified information until receipt of written confirmation of reinstatement and an up-to-date personnel security packet will be furnished with the request for reinstatement of an access authorization. A new Security Acknowledgement will be obtained in all cases. Where personnel security packets are not required, a request for reinstatement must state the level of access authorization to be reinstated and the full name and date of birth of the individual to establish positive identification. A fee, equal to the amount paid for an initial request,